IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN RE THE SEARCH OF:	)	
	)	
GOOGLE DRIVE ACCOUNT	)	
REGISTERED TO EMAIL ADDRESS:	)	
JMORRISON363@GMAIL.COM	)	
GOOGLE, INC.	)	Magistrate No. 17-172M
1600 AMPHITHEATRE PARKWAY	)	**[UNDER SEAL]**
MOUNTAIN VIEW, CALIFORNIA 94043	)	

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Martin Ryan, a Special Agent (SA) with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to assist the Special Agent in Charge, Pittsburgh, Pennsylvania, and have been so employed since July 2004. Prior to my appointment with HSI, I was employed as a United States Border Patrol Agent for approximately five years. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252(a). I have received training in the area of child pornography and child exploitation investigations, and have had the opportunity to observe and review numerous examples of images depicting minors engaged in sexually explicit conduct (as defined in Title 18, United States Code, Section 2256) (hereinafter "child pornography") in a variety of media, including computer media. I have also participated in the execution of numerous search

warrants which involved child exploitation and/or child pornography offenses.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is submitted in support of an application for a search warrant for information contained in or associated with the Google Drive internet cloud based storage site, which is connected to the electronic mail (e-mail) account of **jmorrison363@gmail.com**, controlled by the web-based electronic communication service provider known as Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. As discussed below, the Google Drive and e-mail account which is the subject of this search warrant, **jmorrison363@gmail.com**, was identified through the investigation of an online image sharing website sharing child pornography. As set forth herein, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a), regarding the possession, distribution and receipt of visual depictions involving the use of a minor engaging in sexually explicit conduct, are located within information associated with this e-mail account.

4. The purpose of this application is to search for and seize evidence, fruits and instrumentalities, more particularly described in Attachment A, of violations of Title 18, United States Code, Section 2252(a)(2), which makes it a crime to receive and distribute material depicting the sexual exploitation of a minor and Title 18, United States Code, Section 2252(a)(4)(B), which makes it a crime to possess or access with intent to view material depicting the sexual exploitation of a minor.

5. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines "minor", for purposes of Section 2252, as "any person under the age of

eighteen years". Section 2256 also defines "sexually explicit conduct" for purposes of these sections as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic; or (e) lascivious exhibition of the genitals or pubic area of any person.

6. The statements in this affidavit are based, in part, on my personal observations, my training and experience, and information obtained from other agents, police officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

GOOGLE DRIVE

7. Google Drive is a file hosting service operated by Google, Inc., headquartered in Mountain View, California, that offers cloud storage, file synchronization, personal cloud, and client software. Google Drive allows users to create a special folder on each of their computers, cellular phones and other electronic devices, which Google Drive then synchronizes so that it appears to be the same folder (with the same contents), regardless of which computer or device is used to view it. Files placed in this folder are also accessible through website and mobile phone applications.

8. Google Drive users sign up for an account with a valid e-mail address. Google Drive provides users with a certain amount of free data storage, and if the user wants more storage, the user can pay for it. Users can access Google Drive from anywhere in the world using the Internet. For example, a user may take a photograph from a smartphone, upload that photo to Google Drive, and then erase the photo from the user's phone. The photograph now resides in the user's "cloud." The user can then access his/her Google Drive account from a desktop computer, cellular phone or electronic device and download the photograph to that computer.

9. Another feature of Google Drive is sharing. A Google Drive user can share certain files he/she designates by sending a web link to another user(s). It then gives the additional user(s) access to those particular files.

10. Your Affiant knows that Google Drive maintains records on their users, such as basic subscriber information within the meaning of 18 U.S.C § 2703(c)(2). Furthermore, your Affiant knows that Google Drive keeps and maintains the stored content of user accounts, such as photographs, movies, documents and music within the meaning of the Stored Communications Act. Once the records are received, government investigators will review the records and copy those files that are specified in Attachment B.

PROBABLE CAUSE

11. In September 2015, Homeland Security Investigations (HSI), Cyber Crimes Center (C3), Child Exploitation Investigations Unit (CEIU) became involved in an ongoing child exploitation investigation targeting multiple users of an Internet-based bulletin board dedicated to the advertisement, distribution, and production of child pornography (hereinafter "the investigation"). In October 2015, HSI C3 CEIU began working the investigation with the assistance of the Department of Justice (DOJ), Child Exploitation and Obscenity Section (CEOS). As a result of the investigation, the IP address 73.214.93.95 was identified as having downloaded child pornography from a remote hosting site on August 2, 2016 at 07:08:57 UTC-400. The aforementioned IP address resolves to Comcast customer Dennis MORRISON, 1623 McBride Street, Pittsburgh, PA 15207.

12. On January 26, 2017, HSI Pittsburgh agents and Pittsburgh Police Officers (Zone 4) executed Federal Search Warrant at the residence of Dennis Morrison (DOB: 10/22/1955) and Joel MORRISON (DOB: 11/04/1983) at 1623 McBride Street Pittsburgh, PA 15207.

13. Joel MORRISON was not encountered at the residence at the time of the search warrant. On January 26, 2017, HSI Special Agents (SA) Brandon Wargo and Martin Ryan visited the place of employment for Joel MORRISON, Bob's Autotorium, 1408 River Road, Homestead, PA 15120. Joel MORRISON agreed to speak with the agents without the presence of an attorney, and agreed to be interviewed in an HSI Pittsburgh government-owned vehicle, as other accommodations were not available at the place of employment. The agents advised Joel MORRISON that he was not under arrest, that he was free to leave and return to work, and that any statements would be voluntary. The agents advised Joel MORRISON that a search warrant had been executed at his residence.

14. Joel MORRISON said that he lives at the residence with his father, Dennis Morrison. Joel MORRISON said that he does not have a computer or laptop in the residence, and that he has a tablet in the residence that he has not used for a few years. Joel MORRISON said that while he technically could use his father's laptop to access the internet, he has not done so. Joel MORRISON said that he uses his Samsung Android cell phone to access the internet in his residence, via wireless router. Joel MORRISON provided the agents with his email address, **jmorrison363@gmail.com**.

15. SA Ryan asked Joel MORRISON whether he was familiar with the term "child pornography", and how he would describe it. Joel MORRISON answered, "yes, disgusting". Joel MORRISON then agreed with SA Ryan that "child pornography" could be described as images or recordings of children, under age 18, engaged in sexual acts, either alone or with other individuals. The agents explained that the IP address at the residence through Comcast Cable had been used to access child pornography via the internet.

16. At first, Joel MORRISON said that he had only viewed child pornography or child

exploitation material accidentally on the internet, after receiving unwanted so-called "pop-ups", or unrequested advertising or notifications. After additional questioning, Joel MORRISON admitted that he had viewed child pornography on the internet, having viewed it on his Samsung Android cellphone while using the Comcast internet connection in his residence. Joel MORRISON said that he had been viewing child pornography/child exploitation material on his cell phone for approximately the last six months to one year.

17. Joel MORRISON said that his Samsung Android cell phone was located in his work space inside Bob's Autotorium. Joel MORRISON said that currently there might be one image described as child pornography on his cell phone, that of an approximately 12-13-year-old girl. Joel MORRISON agreed to show HSI Pittsburgh agents the image of child pornography on his cell phone.

18. Joel MORRISON led SA Wargo to his workspace inside Bob's Autotorium, and powered on his cell phone for SA Wargo. Joel MORRISON showed SA Wargo a file located on Joel MORRISON's Google Drive Account, related to his email address **jmorrison363@gmail.com**. Joel MORRISON showed SA Wargo a Google Drive video file, approximately 1-2 minutes in length, dated November 29, 2016, which depicted an approximately 12-year-old, prepubescent female masturbating. After showing SA Wargo the video, Joel MORRISON turned his Samsung Android over to SA Wargo and said, "my life is over". SA Ryan seized the Samsung Android cell phone, pending the application of a search warrant.

19. On January 26, 2017, SA Ryan sent a Preservation Letter to Google, for the Google Drive account for the account associated with **jmorrison363@ gmail.com**, for a period of 90 days. The account is associated with Joel MORRISON. On January 31, 2017, SA Brandon Wargo uploaded the same Preservation Letter to the Google Law Enforcement Request System (LERS).

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

20. Title 18, United States Code, Chapter 121, Sections 2701 through 2712, is entitled the "Stored Communications Act" (SCA). Section 2703 of the SCA sets forth the procedure that federal and state law enforcement officers follow to compel disclosure of various categories of stored electronic information from service providers. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by Section 2711(3)(A)(i) of the SCA. This application is made pursuant to the Stored Communications Act and the Federal Rules of Criminal Procedure.

21. This application seeks a warrant to obtain copies of all files, videos, images, emails, messages, and other information and electronic data that may be found on Google servers which pertain to the following Google Drive account:

a. Google Drive account registered to email address: **jmorrison363@gmail.com**.

CONCLUSION

22. Based upon the information contained in this application and affidavit, there is probable cause to conclude that on the computer systems owned, maintained, and/or operated by Google there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(2), which makes it a crime to receive and distribute material depicting the sexual exploitation of a minor.

23. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment A.

24. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including the

Application, Affidavit, and the Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

25. A separate motion for an order requiring non-disclosure of the search warrant to the subscriber pursuant to Title 18, United States Code, Section 2703(b)(1)(A), and Title 18, United States Code, Section 2705(b), is being filed simultaneously herewith.

MARTIN RYAN
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
this 22nd day of February, 2017.

LISA PUPO LENIHAN
United States Magistrate Judge

ATTACHMENT A

I. DESCRIPTION OF PROPERTY TO BE SEARCHED

1. This warrant applies to information associated with the e-mail account of **jmorrison363@gmail.com**, controlled by the web-based electronic communication service provider known as Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043.

II. SERVICE OF WARRANT AND SEARCH PROCEDURE

1. The officer executing this warrant shall affect service by any lawful method, including faxing the warrant to the location specified in the warrant.

2. To minimize any disruption of computer service to third parties, the officer executing this warrant shall direct the service provider's employees to locate, isolate, and create an exact duplicate of all contents of communications, records, and other information associated with the subscriber account(s) as described in Section III below.

3. The terms "records," "information," "communications," "contents," and "files" include all of the items described in this Attachment in whatever form and by whatever means they may have been created or stored, including, without limitation, any electronic or magnetic form (such as hard drives, floppy disks, CD-ROMs, backup tapes, and printouts or readouts from any such media), and any handmade, mechanical, or photographic form (such as writing, printing, typing, or photocopies).

4. The service provider's employees will provide the exact duplicate in electronic form (or as printouts if the original records are not in electronic form) of the subscriber account files described in Section III below to the agent who serves this search warrant, who need not be present at the location specified in the warrant during the retrieval of records, as permitted in 18 U.S.C. § 2703(g).

5. Law enforcement personnel will thereafter review the information stored in the files and accounts received from the service provider and then identify the relevant communications, records, and information contained in the files as described in Section IV below.

III. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES

1. All electronic mail and electronic data stored and presently contained in, or on behalf of, the following account – **jmorrison363@gmail.com** (hereafter "the subject account") – and any and all other aliases or screen names associated with this account.

2. All existing printouts from original storage of all of the electronic mail described above in Section III (1).

3. All transactional information of all activity of the electronic mail addresses and/or individual accounts described above in Section III (1), including log files, dates, times, methods of connecting ports, dial-ups, and/or locations.

4. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in Section III (1), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, and detailed billing records.

5. All records indicating the services available to subscribers of the electronic mail addresses and/or individual accounts described above in Section III (1).

6. All instant messages stored and presently contained in, or on behalf of, the subject account, and any and all other aliases or screen names associated with this account.

7. Copies of all images, videos, or graphics posted to the service provider's properties, photos, briefcase, or otherwise stored and/or associated with the subject account or any other screen names/email addresses associated with the subject account.

IV. INFORMATION TO BE REVIEWED AND IDENTIFIED BY LAW ENFORCEMENT PERSONNEL

1. Upon receipt of the information described in Section III above, law enforcement personnel will identify and copy the following information:

   a. From the communications, electronic data, records, and information described above in Section III, all electronic mail, clubs, web pages, or other communications and account contents, and all transactional and subscriber information from the subject account and any and all other aliases or screen names associated with this account, and e-mail sent to, from, or through such subscriber accounts, whether or not the electronic mail or account contents have been retrieved, that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252, as well as all of the records and information described above in Section III (1-7) that constitute

evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252.